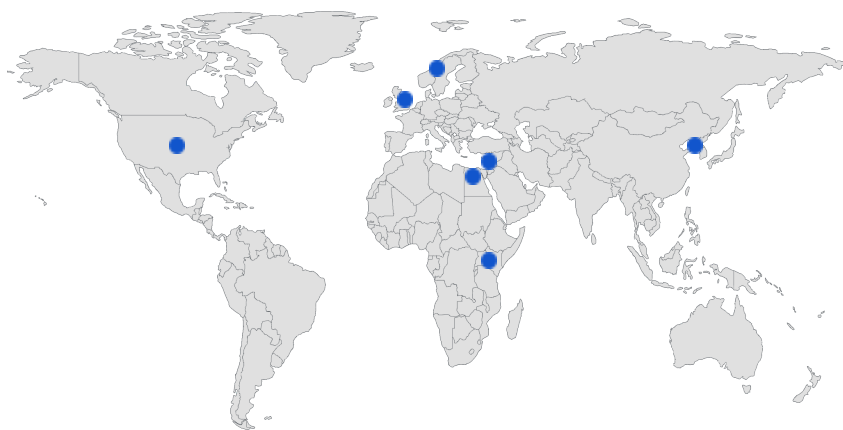


Threat Intel Report: July 24-30

Countries



Top Tags

SiegedSec

FIN7

Lazarus Group

MoveIT

Government

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

📈 26% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

📈 58% [CVE-2022-22965](#)

- a RCE vulnerability in Spring programs ("Spring4Shell")

📈 41% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

Anonymous Sudan targets Kenyan sites

+Kenya +DDoS

- DDoS attacks on Kenya reached a record high on July 31, coinciding with Anonymous Sudan's targeting of the country. DDoS attacks peaked at a maximum RPS 445% higher than anything we've previously seen in the country.

Lebanon sees spike in bad bot attacks

+Lebanon +Bad Bots

- Bot attacks on Lebanon-based sites rose almost 7,000% on July 30th. Attacks came from just 219 distinct IPs, mostly based in Germany and the US.

Recent Cyber Threats

SiegedSec leaks NATO data

+NATO +Government +SiegedSec

- The hacktivist group [SiegedSec](#) breached NATO's systems, leading to a significant data leak. The group claims that the action was a protest against NATO's activities and aims to expose the organization's secrets.

Title

+Financial Services +OSS Attack +FIN7

- The banking sector experienced its [first-ever open-source software](#) (OSS) supply chain attack. The attack was orchestrated by the threat actor group FIN7, which exploited a vulnerability in the Apache Log4j library, affecting numerous banks and financial institutions.

New ransomware targeting Middle Eastern government organizations

+Middle East +Government +Ransomware

- Middle Eastern government organizations have been targeted by new [ransomware](#) attacks that appear to be politically motivated. The attacks are sophisticated and targeted, suggesting the involvement of state-sponsored actors.

Critical security flaw found in MicroTik routers

+Computing & IT

- A critical severity super admin privilege elevation flaw has been discovered in over 900,000 [MikroTik](#) RouterOS routers. This flaw could allow attackers with an existing admin account to elevate their privileges and potentially take full control over a device.

Peloton treadmills exposed to malware and DDoS

+Exercise

- [Peloton](#) treadmills were found to have security vulnerabilities that left them susceptible to malware and DDoS attacks. The vulnerabilities were found in the operating system, applications, and have potential for malware installation, raising concerns about the security of internet-connected gym equipment.

Security flaw discovered in Metabase software

+Computing & IT

- A major security flaw has been discovered in [Metabase](#), a popular business intelligence and data visualization software package. The flaw, which could result in preauthenticated remote code execution on affected installations, has been addressed in the latest versions of the software.

Data Breaches

Norway targeted by unknown cyber attack

+Norway +Government

- [Norway's](#) government ministries were targeted in a sophisticated cyber attack. The attack was detected early and measures were taken to counter it, but the extent of the damage is still being assessed.

Hacker claims to have 2M Egyptian records for sale

+Egypt +Government

- An unknown hacker claims to have stolen two million data records from the [Egyptian Ministry of Health and Population](#). The stolen data reportedly includes comprehensive personal patient information, and the hacker is attempting to sell this data on a hacker forum.

Ortivus cyberattack affects UK patient record systems

+UK +Healthcare

- [Ortivus](#), a provider of electronic patient record systems, experienced a cyber attack that affected its UK customer systems. The electronic patient records are currently unavailable and are being handled using manual systems, but no patients have been directly affected.

Government services firm Maximus loses 11M people's records in MoveIT attack

+Government +MoveIT

- Government services provider [Maximus](#) revealed that the personal information of up to 11 million individuals was stolen in the MoveIT cyberattack. The company is currently working on investigating and remedying the incident, which is expected to incur expenses of approximately \$15 million.

Crypto company CoinsPaid loses \$37M in suspected Lazarus attack

+Cryptocurrency +Lazarus Group +North Korea

- Cryptopayment service provider [CoinsPaid](#) suffered a cyber attack that resulted in the theft of \$37.2 million worth of cryptocurrency. The company attributes the attack to the North Korea-linked APT Lazarus group, and is currently working to restore its systems and recover data.

Policies & Regulations

US SEC implements new cyberattack disclosure rules

+US +Government

- The [U.S. Securities and Exchange Commission](#) (SEC) has implemented new rules that mandate publicly traded companies to disclose cyberattacks within four days of determining them as material incidents. These rules require companies to provide detailed information about the cyberattack, including its nature, scope, and timing, and are set to take effect in December.

Imperva Protection

Imperva provides comprehensive digital security solutions, including protection against threats to web applications and APIs– including security vulnerabilities, fraud, and bad bots, data security solutions, and security against disruptive network- and application-level DDoS attacks.



By Phone:
650-345-9000



By Fax:
888-611-7282

By mail:

Imperva Headquarters
One Curiosity Way, Suite
203 San Mateo, CA 94403